Exhibit 22

Excerpts of SW-SEC00151673

From:	Pierce, Kellie [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=0150EF14C7A24CB1A0E08EC9FCB06424-PIERCE, KEL]
Sent:	6/28/2019 8:37:58 PM
To:	Fu, Ikong [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=f7c378044ca141209da12d5a5874cff4-Fu, Ikong]; Fujii, Ross [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=f2007a77afcc470289c878f02563304e-Fujii, Ross]
CC:	Hansen, Jim [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d23033ce6fe14dea908e533ef92fbca3-Hansen, Jim]; Brown, Timothy [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a1bcd95116e84d6692dd89f9d55c5b7a-Brown, Timo]; Johnson, Rani [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0ee57945f15e47b3abaa99a59170ad3f-Johnson, Ra]
Subject:	FedRAMP - Security & Compliance Preliminary Review
Attachments:	FedRAMP_Security_Controls_Baseline as of 06282019.xlsx

Good afternoon,

I've performed a preliminary review of the 325 FedRAMP Moderate controls; my takeaway is that 94% (304) of the controls will require a moderate to significant level of effort to implement.

Also, I would like to share that the work will be required from these groups within SolarWinds: Product Management, Engineering, SRE/DevOps, Facilities and DOIT.

High level based on Green/Yellow/Red:

Program/Practice in place	21	6%
Program/Practice *may* be in place but requires detailed review	106	33%
No program/practice in place	198	61%
TOTALS	**325**	**100%**

Breakdown by Control type and Green/Yellow/Red:

		Program/Practice in place	Program/Practice *may* be in place but requires detailed review	No program/practice in place	
CONTROLS		🟩	🟨	🟥	**Total**
AC	ACCESS CONTROL	2	18	23	**43**
AT	AWARENESS AND TRAINING	0	5	0	**5**
AU	AUDIT AND ACCOUNTABILITY	0	1	18	**19**
CA	SECURITY ASSESSMENT AND AUTHORIZATION	2	3	10	**15**
CM	CONFIGURATION MANAGEMENT	1	7	18	**26**
CP	CONTINGENCY PLANNING	1	19	4	**24**
IA	IDENTIFICATION AND AUTHENTICATION	0	7	20	**27**
IR	INCIDENT RESPONSE	13	3	2	**18**
MA	MAINTENANCE	0	1	10	**11**
MP	MEDIA PROTECTION	0	0	10	**10**

PE	PHYSICAL AND ENVIRONMENTAL PROTECTION	0	14	6	**20**
PL	PLANNING	0	4	2	**6**
PS	PERSONNEL SECURITY	0	0	9	**9**
RA	RISK ASSESSMENT	0	6	4	**10**
SA	SYSTEM AND SERVICES ACQUISITION	2	8	12	**22**
SC	SYSTEM AND COMMUNICATIONS PROTECTION	0	3	29	**32**
SI	SYSTEM AND INFORMATION INTEGRITY	0	7	21	**28**
	TOTAL	**21**	**106**	**198**	**325**

Please let me know if I can provide any detailed information.
Thank you,
Kellie

solarwinds
Kellie Pierce | Security & Compliance Sr. Program Manager | **SolarWinds**
Office: 512.498.6248

DOCUMENT PRODUCED IN NATIVE FORMAT

16	**AC-06**	ACCESS CONTROL	**AC-6**	LEAST PRIVILEGE	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2. References: None.	**Process**					KP 6/27: This is included in the Access/Security Guidelines document. An audit that this is in place has never been performed.
17	**AC-06 (01)**	ACCESS CONTROL	**AC-6 (1)**	LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS	The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information]. Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.	**Process**					KP 6/27: We have no explicit authorization policy, nor is this documented that I am aware of for the company or individual products
18	**AC-06 (02)**	ACCESS CONTROL	**AC-6 (2)**	LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non- privileged accounts or roles, when accessing nonsecurity functions. Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.	**Process**					KP 6/27: This is included in the Access/Security Guidelines document. An audit that this is in place has never been performed.
19	**AC-06 (05)**	ACCESS CONTROL	**AC-6 (5)**	LEAST PRIVILEGE | PRIVILEGED ACCOUNTS	The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.	**Process**					KP 6/27: We have no explicit restriction policy, nor is this documented that I am aware of for the company or individual products
20	**AC-06 (09)**	ACCESS CONTROL	**AC-6 (9)**	LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS	The information system audits the execution of privileged functions. Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.	**Product**	**No**	**No**	**No**	**No**	KP 6/27: Agree with PM. There is currently no audit
21	**AC-06 (10)**	ACCESS CONTROL	**AC-6 (10)**	LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.	**Product**	**Yes**	**Yes?**	**Yes**	**Yes?**	KP 6/27: This has not been tested/audited, nor is a policy documented.
22	**AC-07**	ACCESS CONTROL	**AC-7**	UNSUCCESSFUL LOGON ATTEMPTS	The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.	**Product**	**No?**	**Partial**	**No?**	**No?**	KP 6/27: Some IT systems have this enabled but it is not consistant across the products

32	**AC-17 (03)**	ACCESS CONTROL	**AC-17 (3)**	REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS	The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points. Supplemental Guidance: Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections. Related control: SC-7.	**Product**	**No**	**No**	**No**	**No**	KP 6/27: IT does manage remote access but "all" would need to be audited to confirm.
33	**AC-17 (04)**	ACCESS CONTROL	**AC-17 (4)**	REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS	The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and (b) Documents the rationale for such access in the security plan for the information system. Supplemental Guidance: Related control: AC-6.	**Process**					KP 6/27: I do not believe this is documented.
34	**AC-17 (09)**	ACCESS CONTROL	**AC-17 (9)**	REMOTE ACCESS | DISCONNECT / DISABLE ACCESS	The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [Assignment: organization-defined time period]. Supplemental Guidance: This control enhancement requires organizations to have the capability to rapidly disconnect current users remotely accessing the information system and/or disable further remote access. The speed of disconnect or disablement varies based on the criticality of missions/business functions and the need to eliminate immediate or future remote access to organizational information systems.	**Product**	**No?**	**No?**	**No?**	**No?**	KP 6/27: Agree with PM- this is not in place for any products and may be somewhat in place for IT managed assets
35	**AC-18**	ACCESS CONTROL	**AC-18**	WIRELESS ACCESS	The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections. Supplemental Guidance: Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. Related controls: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4.	**Process**					KP 6/27: We have some wireless requirements in the Access/Security guidelines howevver they need to be reviewed against the FedRAMP requirements
36	**AC-18 (01)**	ACCESS CONTROL	**AC-18 (1)**	WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION	The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption. Supplemental Guidance: Related controls: SC-8, SC-13.	**Product**	**N/A?**	**N/A?**	**N/A?**	**N/A?**	KP 6/27: We have some wireless requirements in the Access/Security guidelines howevver they need to be reviewed against the FedRAMP requirements
37	**AC-19**	ACCESS CONTROL	**AC-19**	ACCESS CONTROL FOR MOBILE DEVICES	The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems. Supplemental Guidance: A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-	**Process**					KP 6/27: The company does not have a policy on non-network devices connecting to the network.
38	**AC-19 (05)**	ACCESS CONTROL	**AC-19 (5)**	ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION	The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices]. Supplemental Guidance: Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields. Related controls: MP-5, SC-13, SC-28. References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164.	**Process**					KP 6/27: The company does not have an access control for mobile devices
39	**AC-20**	ACCESS CONTROL	**AC-20**	USE OF EXTERNAL INFORMATION SYSTEMS	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems. Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the	**Process**					KP 6/27: Procurement has a process in place for T& C and Data Processing Addendum
40	**AC-20 (01)**	ACCESS CONTROL	**AC-20 (1)**	USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE	The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.	**Process**					KP 6/27: The company has some Data Loss Prevention montiring however no hard blocks on information. This is a will take significant change.

41	**AC-20 (02)**	ACCESS CONTROL	**AC-20 (2)**	USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES	The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems. Supplemental Guidance: Limits on the use of organization-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.	**Process**	KP 6/27: There is no policy around portable storage devices
42	**AC-21**	ACCESS CONTROL	**AC-21**	INFORMATION SHARING	The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.	**Process**	6/27 KP: authorized v.s unauthorized users has not been defined and policies are not fully comprehensive to meet this control
43	**AC-22**	ACCESS CONTROL	**AC-22**	PUBLICLY ACCESSIBLE CONTENT	The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.	**Process**	6/27 KP: We have a communication process in place with approval gates (marketing/legal) however I am unsure if this is clearly documented.
44	**AT-01**	AWARENESS AND TRAINING	**AT-1**	SECURITY AWARENESS AND TRAINING POLICY ANDPROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current:	**Process**	KP 6/27: We have incident commander training however, not a security training/awareness program in place
45	**AT-02**	AWARENESS AND TRAINING	**AT-2**	SECURITY AWARENESS TRAINING	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter. Supplemental Guidance: Organizations determine the appropriate content of security awareness training and security awareness techniques	**Process**	KP 6/27: We have incident commander training however, not a security training/awareness program in place
46	**AT-02 (02)**	AWARENESS AND TRAINING	**AT-2 (2)**	SECURITY AWARENESS | INSIDER THREAT	The organization includes security awareness training on recognizing and reporting potential indicators of insider threat. Supplemental Guidance: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures.	**Process**	KP 6/27: We have incident commander training however, not a security training/awareness program in place
47	**AT-03**	AWARENESS AND TRAINING	**AT-3**	ROLE-BASED SECURITY TRAINING	The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter. Supplemental Guidance: Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access.	**Process**	KP 6/27: We have incident commander training however, not a security training/awareness program in place
48	**AT-04**	AWARENESS AND TRAINING	**AT-4**	SECURITY TRAINING RECORDS	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [Assignment: organization-defined time period]. Supplemental Guidance: Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3, PM-14.	**Process**	KP 6/27: We have incident commander training however, not a security training/awareness program in place
49	**AU-01**	AUDIT AND ACCOUNTABILITY	**AU-1**	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy [Assignment: organization-defined frequency]; and	**Process**	KP 6/27: There is no audit / accountability practice in place. This is undeway for SOX assets.

90	**CM-04**	CONFIGURATION MANAGEMENT	**CM-4**	SECURITY IMPACT ANALYSIS	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. Supplemental Guidance: Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems. Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2.	**Process**					6/27 KP: There may be some change control but unknown/not currently audited
91	**CM-05**	CONFIGURATION MANAGEMENT	**CM-5**	ACCESS RESTRICTIONS FOR CHANGE	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover). Related controls: AC-3, AC-6, PE-3.	**Process**					6/27 KP: There may be some change control but unknown/not currently audited
92	**CM-05 (01)**	CONFIGURATION MANAGEMENT	**CM-5 (1)**	ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING	The information system enforces access restrictions and supports auditing of the enforcement actions. Supplemental Guidance: Related controls: AU-2, AU-12, AU-6, CM-3, CM-6.	**Product**	**No?**	**No**	**No?**	**No?**	6/27/KP: Agree with PMs - no enforcement in lace
93	**CM-05 (03)**	CONFIGURATION MANAGEMENT	**CM-5 (3)**	ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS	The information system prevents the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. Supplemental Guidance: Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers, and basic input output system (BIOS) updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures, is a method of code authentication. Related controls: CM-7, SC-13, SI-7.	**Product**	**No?**	**No?**	**No?**	**No?**	6/27 KP: No prohibition for software installed
94	**CM-05 (05)**	CONFIGURATION MANAGEMENT	**CM-5 (5)**	ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES	The organization: (a) Limits privileges to change information system components and system-related information within a production or operational environment; and (b) Reviews and reevaluates privileges [Assignment: organization-defined frequency]. Supplemental Guidance: In many organizations, information systems support multiple core missions/business functions. Limiting privileges to change information system components with respect to operational systems is necessary because changes to a particular information system component may have far-reaching effects on mission/business processes supported by the system where the component resides. The complex, many-to-many relationships between systems and mission/business processes are in some cases, unknown to developers. Related control: AC-2.	**Process**					6/27 KP: No known privledge limitations
95	**CM-06**	CONFIGURATION MANAGEMENT	**CM-6**	CONFIGURATION SETTINGS	The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and	**Process**					6/27 KP: No known uniform controls for config settings.
96	**CM-06 (01)**	CONFIGURATION MANAGEMENT	**CM-6 (1)**	CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION	The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system components]. Supplemental Guidance: Related controls: CA-7, CM-4.	**Process**					6/27 KP: No known uniform controls for config settings.

263	**SA-11 (01)**	SYSTEM AND SERVICES ACQUISITION	**SA-11 (1)**	DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS	The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis. Supplemental Guidance: Static code analysis provides a technology and methodology for security reviews. Such analysis can be used to identify security vulnerabilities and enforce security coding practices. Static code analysis is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static analysis can provide clear remediation guidance along with defects to enable developers to fix such defects. Evidence of correct implementation of static analysis can include, for example, aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were fixed. An excessively high density of ignored findings (commonly referred to as ignored or false positives) indicates a potential problem with the analysis process or tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.	**Process**					6/28 KP: Checkmarx used for some products; beginning of program in the works
264	**SA-11 (02)**	SYSTEM AND SERVICES ACQUISITION	**SA-11 (2)**	DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES	The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service. Supplemental Guidance: Applications may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat and vulnerability analyses of information systems, system components, and information system services prior to delivery are critical to the effective operation of those systems, components, and services. Threat and vulnerability analyses at this phase of the life cycle help to ensure that design or implementation changes have been accounted for, and that any new vulnerabilities created as a result of those changes have been reviewed and mitigated. Related controls: PM-15, RA-5.	**Process**					6/28 KP: Program in the works.
265	**SA-11 (08)**	SYSTEM AND SERVICES ACQUISITION	**SA-11 (8)**	DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS	The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis. Supplemental Guidance: Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to help to ensure that security functionality performs in the manner in which it was designed. A specialized type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies derive from the intended use of applications and the functional and design specifications for the applications.	**Process**					6/28 KP: No hard requirements known
266	**SC-01**	SYSTEM AND COMMUNICATIONS PROTECTION	**SC-1**	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy [Assignment: organization-defined frequency]; and 2. System and communications protection procedures [Assignment: organization-defined frequency]. Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	**Process**					6/28 KP: Not in place to my knowledge
267	**SC-02**	SYSTEM AND COMMUNICATIONS PROTECTION	**SC-2**	APPLICATION PARTITIONING	The information system separates user functionality (including user interface services) from information system management functionality. Supplemental Guidance: Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls. Related controls: SA-4, SA-8, SC-3. References: None	**Product**	**Yes?**	**Yes?**	**Yes?**	**Yes?**	6/28 KP: Would need review / this is not in place for Loggly. Unknown for Pingdom. AO and Papertrail - per SOX (it is in place)